IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, **Plaintiff,** **vs.** **KEITH B. NODEN,** **Defendant.**	**8:16CR283** **MEMORANDUM AND ORDER**

This matter is before the Court on the Findings and Recommendation, ECF No. 30, issued by Magistrate Judge F.A. Gossett, III, recommending that the Motion to Suppress, ECF No. 23, filed by the Defendant, Keith Noden ("Defendant"), be denied. Defendant filed an Objection to the Findings and Recommendation and a brief in support, ECF No. 33, as allowed by 28 U.S.C. § 636(b)(1)(C) and NECrimR 59.2(a). The Government did not respond. For the reasons set forth below, the Findings and Recommendation will be adopted and the Motion to Suppress will be denied.

BACKGROUND

Defendant is charged in the Indictment, ECF No. 1, with affecting interstate commerce by means of knowingly receiving child pornography on his laptop computer in violation of 18 U.S.C. § 2252A(a)(2).

On or about April 13, 2016, Darin Morrissey ("Affiant"), a Sarpy County Sheriff's Detective working with the Federal Bureau of Investigation ("FBI") Cyber Crimes Task Force, began an investigation into peer-to-peer file-sharing computer software used to download digital files from other users within the peer-to-peer software network. Such

file-sharing networks are commonly used to share and download files containing images of child pornography. Affiant initiated his investigation by utilizing an automated software program called "Grid Cop." Grid Cop is shared by child exploitation investigation entities and it browses the various peer-to-peer program networks to identify Internet Protocol ("IP") addresses "that are seen having child-notable child pornography files available for sharing" and generates an activity log of its findings. ECF No. 32, Page ID 100. Whenever an individual user shares files containing child pornography via peer-to-peer computer software, Grid Cop is potentially logging that activity and identifying it by the user's associated computer IP address.

When an investigator observes that Grid Cop has identified a particular IP address as having shared child pornography files, the investigator is able to extract the hash[1] values associated with each file and convert them into Secure Hash Algorithm Version 1 ("SHA-1")[2] values. ECF No. 32, Page ID 102. SHA-1 values are a particular type of hash value,[3] and law enforcement agencies maintain their own libraries of files containing child pornography identified by SHA-1 values. *Id*. This allows the investigator to extract the hash values from files identified by Grid Cop as containing child pornography, convert them to SHA-1 values, and check law enforcement libraries for a matching SHA-1 value. *Id*. If the converted SHA-1 values match the SHA-1

[1] Hash values "are an algorithmic calculation that yields an alphanumeric value for a file." *United States v. Stevenson*, 727 F.3d 826, 828 (8th Cir. 2013).

[2] SHA-1 values are a "digital fingerprint of a computer file" and consist of a "32-digit number that is calculated for a file and unique to it." *United States v. Glassgow*, 682 F.3d 1107, 1110 (8th Cir. 2012).

[3] SHA-1 values were "developed by the National Institute of Standards and Technology, along with the National Security Agency." *United States v. Warren*, No. 4:08 CR189RWS, 2008 WL 3010156, at *1 (E.D. Mo. July 24, 2008), report and recommendation adopted, No. 4:08CR189RWS, 2008 WL 4512524 (E.D. Mo. Sept. 30, 2008).

values of a file within law enforcement libraries, the investigator downloads the file from the library to confirm the illicit content in the suspect file provided by Grid Cop. Investigator Dishaw testified that this conversion and comparison process is highly accurate and comparable to the standard DNA comparison accuracy rate. *Id*.

According to the Grid Cop software, Affiant observed that IP address 68.229.178.123 had shared, and been in possession of, files containing child pornography on more than ten separate occasions between February 7, 2016, and April 15, 2016. Affiant converted the hash values associated with three of the files to SHA-1 values, located the matching files within the law enforcement file library, downloaded them, and confirmed that they contained child pornography. Affiant also determined that the IP address associated with the illegal files was leased to the Defendant from Cox Communications. Affiant stated the foregoing facts, truthfully, in an affidavit submitted in support of a search warrant for Defendant's home and personal computer.

The affidavit supporting probable cause for the search also included certain statements that were false. The affidavit stated that Affiant was able to use an undercover computer to participate in the same peer-to-peer file-sharing network as Defendant; that Affiant connected directly to Defendant's IP address; that Affiant browsed the available shared files; and that Affiant downloaded certain files containing child pornography. The Government acknowledged that, in fact, Affiant never directly browsed or downloaded any files made available from Defendant's IP address via a peer-to-peer file-sharing network. Thus, any statements in the affidavit that asserted such a direct connection, browse, and download had been accomplished were untrue.

Affiant submitted the affidavit; obtained a search warrant; executed it on July 27, 2016; and a laptop computer was recovered from Defendant's bedroom. While no files containing child pornography were found on the computer, the Government observed several explicit keyword searches associated with child pornography. At the time of the search, the Defendant also explained that he had deleted all of the child pornography files from his computer and he admitted installing the "E Mule" file-sharing program to access and view child pornography.

Defendant moves to suppress all evidence obtained during the search, including his incriminating statements, as fruit of the poisonous tree, *i.e.*, a search warrant issued absent probable cause in violation of the Fourth Amendment. After receiving briefs and holding a *Franks* hearing, the Magistrate Judge recommended that the Court deny the Motion to Suppress. The Magistrate Judge reasoned that the false statements in the affidavit were not made deliberately and knowingly, or with reckless disregard for the truth pursuant to *Franks v. Delaware*, 438 U.S. 154, 171-72 (1978). The Magistrate Judge further concluded that absent the false statements, the affidavit still supported probable cause for the warrant to issue. The Magistrate Judge also concluded that Defendant's incriminating statements made during the search would not be subject to the exclusionary rule because they were too attenuated from the asserted Fourth Amendment violation. Finally, the Magistrate Judge found, over Defendant's objection, that the files listed in paragraphs 37 and 38, and the entirety of paragraph 41, were true statements in the supporting affidavit. Defendant objects to each of the foregoing findings.

STANDARD OF REVIEW

Under 28 U.S.C. § 636(b)(1)(C), the Court must make a de novo determination of those portions of the findings and recommendation to which the Defendant has objected. The Court may accept, reject, or modify, in whole or in part, the Magistrate Judge's findings or recommendation. The Court may also receive further evidence or remand the matter to the Magistrate Judge with instructions.

DISCUSSION

I. False Statements

Defendant contends that the false statements contained in the warrant affidavit render the search warrant, and the search performed pursuant to the warrant, invalid under *Franks v. Delaware*, 438 U.S. 154 (1978), and the Fourth Amendment. "To void a search warrant under *Franks*, a defendant must show by a preponderance of evidence that (1) the affiant included in the warrant affidavit 'a false statement knowingly and intentionally, or with reckless disregard for the truth,' and (2) 'the affidavit's remaining content is insufficient to establish probable cause.'" *United States v. Finley*, 612 F.3d 998, 1002 (8th Cir. 2010) (quoting *Franks*, 438 U.S. at 155-56).

The Magistrate Judge found, and the Government concedes, that the following statements were untrue and they were redacted from the affidavit:

> When using the manual method, Investigator Morrissey connected to an internet protocol (IP) address using P2P [peer-to-peer] software. Investigator Morrissey requested, through P2P software, to browse the "Shared File" folder at that address. Investigator Morrissey was given a listing of multiple files which were available advertisements from computers with child pornography and/or child sexual abuse images or videos available for sharing. Investigator Morrissey exported the multiple files with their respective SHA-1 values and/or Gnutella hash values in the publicly available folder (also known as a "shared folder") and loaded them into software shared by the Child Exploitation Investigative Entities to

> ascertain if any identified child pornography images and/or videos were present.

Affidavit of Investigator Darin Morrissey, No. 8:16MJ229, ¶ 32, ECF No. 1, Page ID 14-15. The following untrue statements were also redacted:

> Using law enforcement information obtained from previous investigations, Investigator Morrissey [Affiant] connected to Internet Protocol (IP) address 68.229.178.123 using the P2P [peer-to-peer] software. Investigator Morrissey requested, through P2P software, to browse the "Shared File" folder at that address, Investigator Morrissey was given a listing of multiple files which contained file names indicative of child pornography and was able to download the below listed files: . . . .

Affidavit of Investigator Darin Morrissey, No. 8:16MJ229, ¶ 37, ECF No. 1, Page ID 16. The above statements from paragraphs 32 and 37 of the warrant affidavit (collectively, the "Redacted Statements") were redacted because they inaccurately alleged that Affiant accomplished a direct connection to Defendant's IP address via peer-to-peer file-sharing software, browsed the shared files, and downloaded those files.

Defendant objects to the Magistrate Judge's findings, arguing that the file information listed in paragraphs 37 and 38 was also untrue and should have been redacted as well. Affiant testified that he obtained the files and their identifying hash values through the Grid Cop software, converted them to SHA values, located the corresponding files within the FBI Cyber Crimes Task Force library network, and confirmed the matching library files contained child pornography. ECF No. 32, Page ID 130-33. Defendant argues that the files were not accurately listed in paragraph 37 or 38 of the affidavit, however, because the redacted language in paragraph 37 preceded the list. Although this language mischaracterized the way in which the files and their corresponding information were obtained by the Government, it does not mean the files

or their corresponding information were untrue or inaccurate. As previously noted, Affiant discovered the files and their information, including hash values, via Grid Cop and stated as much in the affidavit. ECF No. 32 Page ID 142-43. Therefore, the only inaccuracy was the method used to obtain the file information, not the information itself, and any statements made to that effect were appropriately redacted from paragraphs 32 and 37. Defendant has not demonstrated that the file information itself was untrue or inaccurate.

The Magistrate Judge also found that paragraph 41 of the affidavit was a factually accurate statement and did not redact it. Paragraph 41 states:

> The files were downloaded and observed by Investigator Morrissey [Affiant] and confirmed to be child pornography as defined in Title 18, United States Code, Section 2256. The pornographic images and/or videos described herein were publicly advertised via the Internet to Investigator Morrissey, and those public advertisements originated from a cable modem inside the residence known as 7523 S. 75th Ave. La Vista, Nebraska 68128.

Aff. ¶ 41, ECF No. 1 in Case No. 8:16mj229, Page ID 19. Defendant asserts that the download referenced in paragraph 41 referred to a direct download from Defendant's computer via peer-to-peer file-sharing software. Affiant and Investigator Dishaw, however, testified that the download referenced in paragraph 41 does not refer to a direct download. ECF No. 32, Page ID 105-06 & Page ID 132-34. Rather, it refers to the download Affiant made from law enforcement libraries in order to confirm the content of the files identified by Grid Cop as likely containing child pornography. *Id*. Defendant has not sufficiently demonstrated otherwise. The statements in paragraph 41 are, therefore, not subject to redaction.

Accordingly, the Court adopts the Magistrate Judge's finding that the Redacted Statements are untrue and must be redacted from the affidavit. Moreover, the Court adopts the Magistrate Judge's findings that the file information listed in paragraphs 37 and 38, and the entirety of paragraph 41 are factually accurate and not subject to redaction from the affidavit.

II. Probable Cause

The Court adopts the Magistrate Judge's conclusion that absent the Redacted Statements, the warrant affidavit supports a finding of probable cause consistent with the Fourth Amendment. Accordingly, It is not necessary to evaluate whether Affiant made the false statements "knowingly and intentionally, or with reckless disregard for the truth" under *Franks* because the "false statements [are not] necessary to a finding of probable cause." *Franks*, 438 U.S. at 156.

"[T]he existence of probable cause depends on whether, in the totality of the circumstances, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Keys*, 721 F.3d 512, 518 (8th Cir. 2013). "The duty of a reviewing court is 'simply to ensure that the magistrate had a substantial basis for . . . concluding that probable cause existed.'" *United States v. Miknevich*, 638 F.3d 178, 182 (6th Cir. 2011) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). In *United States v. Beatty*, the Sixth Circuit Court of Appeals affirmed a magistrate judge's finding of probable cause when the affidavit contained: (1) file names with "highly graphic references" to "sexual acts involving children," and (2) a statement that "the SHA 1 values belonging to the files on [the defendant's] computer bore the same SHA 1 values as known child pornography in the . . . Task Force database." 437 Fed. App'x

185, 188 (6th Cir. 2011). The same information was stated in the warrant affidavit at issue in this case.

First, the unredacted file information in paragraph 37 of the affidavit lists the file information for three separate files and each includes explicit language referring to children nine to fourteen years old. Second, paragraph 38 of the affidavit explained that the converted SHA-1 values associated with the files matched the SHA-1 values of files maintained in the FBI Cyber Crimes Task Force library. Using Grid Cop, Affiant discovered that Defendant's computer IP address had previously shared, and necessarily possessed, suspect files containing child pornography on more than ten separate occasions. Affiant took the files' identifying hash values provided by Grid Cop and converted them to SHA-1 values. Affiant then compared the converted SHA-1 values to those maintained in law enforcement libraries and discovered a match. Affiant downloaded the file with matching SHA-1 values from the collective law enforcement library and confirmed that the file contained child pornography. These true and accurate facts were stated in the warrant affidavit and sufficiently established "a fair probability," that child pornography would be found on Defendant's computer.

Defendant contends that the factual statements in the affidavit are not sufficient to support a finding of probable cause because the information provided by Grid Cop is analogous to an unreliable anonymous tip. It is Defendant's burden to show by a preponderance of the evidence that probable cause is lacking absent the false statement. Yet, Defendant cites no authority for his claim that Grid Cop is inherently unreliable or that a direct download of the file is necessary to establish probable cause. *See, e.g.*, *United States v. Thomas*, No. 5:12-CR-37, 2013 WL 6000484, at *23 (D. Vt.

Nov. 8, 2013), aff'd, 788 F.3d 345 (2d Cir. 2015) (pointing out that the defendant has not provided authority or sufficiently demonstrated that only a direct download can support a finding of probable cause). Accordingly, the false statements in paragraphs 32 and 37 alleging Affiant made a direct connection to Defendant's computer and downloaded files containing child pornography were not necessary to a finding of probable cause.

It is established law that, "An anonymous tip . . . is insufficient in itself to support a finding of probable cause." *United States v. Wells*, 223 F.3d 835, 839 (8th Cir. 2000). Grid Cop, however, is not anonymous. The United States Supreme Court explained that "an anonymous tip alone seldom demonstrates the informant's basis of knowledge or veracity," as opposed to a "known informant whose reputation can be assessed and who can be held responsible if her allegations turn out to be fabricated." *Florida v. J.L.*, 529 U.S. 266, 270 (2000). Grid Cop is a known source that operates with known computer software susceptible to ascertainable statistics regarding accuracy. Its basis of knowledge is clearly demonstrated and its veracity may be readily checked. As such, the warrant affidavit did not rely on an anonymous tip; it contained information from a known source used by specialized law enforcement personnel tasked with investigating child pornography activity.

Defendant has also not persuaded the Court that Grid Cop is unreliable. The affidavit itself demonstrated that Affiant corroborated some of the information provided by Grid Cop, and "[a]n informant may . . . be considered reliable if the information he or she supplies 'is at least partially corroborated' by other sources." *United States v. Buchanan*, 574 F.3d 554, 562 (8th Cir. 2009) (quoting *United States v. Humphreys*, 982 F.2d 254, 258 n.2 (8th Cir. 1992)). Furthermore, "[i]f information from an informant is

shown to be reliable because of independent corroboration, then it is a permissible inference that the informant is reliable and that therefore other information that the informant provides, though uncorroborated, is also reliable." *Id.* (quoting *United States v. Williams*, 10 F.3d 590, 593 (8th Cir. 1993)).

Affiant took the hash values of three suspect files provided by Grid Cop, converted them to SHA values, and checked them against law enforcement libraries to confirm they contained child pornography. This method of conversion has a rate of accuracy on par with DNA matching. ECF No. 32, Page ID 102-03; *see, e.g.*, *United States v. Glassgow*, 682 F.3d 1107, 1110 (8th Cir. 2012) (recognizing expert testimony that SHA-1 value matching methods have a 99.9999% accuracy rate); *United States v. Dunn*, 777 F.3d 1171, 1173 (10th Cir. 2015) ("Separate files with the same SHA–1 values will have identical content"). Thus, Affiant corroborated at least some of the information provided by Grid Cop and the only evidence of unreliability proffered by Defendant is one instance of inaccuracy unrelated to this case. On cross-examination Investigator Mark Dishaw stated he experienced one issue of inaccuracy in the seven years he has worked with Grid Cop. With this, Defendant has not demonstrated that Grid Cop is either an anonymous or unreliable source and has, ultimately, failed to demonstrate by a preponderance of the evidence that probable cause was lacking absent the false statements in the warrant affidavit.

CONCLUSION

Although Affiant included false statements of fact in the affidavit submitted to support the issuance of a warrant for the search of Defendant's home, those false statements were not necessary to a finding of probable cause. Affiant's remaining

truthful statements based on the information provided by Grid Cop were sufficient to support such a finding of probable cause. Therefore, the Court adopts the Magistrate Judge's conclusion that the affidavit, excluding the Redacted Statements, was sufficient to support a finding of probable cause. Accordingly, it is not necessary for the Court to evaluate whether the Redacted Statements were made "knowingly and intentionally, or with reckless disregard for the truth." *Franks*, 438 U.S. at 156. Nor is it necessary for the Court to evaluate whether the evidence obtained from the search is too attenuated from any Fourth Amendment violation because no such violation has been found.

IT IS ORDERED:

1. The Findings and Recommendation, ECF No. 30, issued by United States Magistrate Judge F.A. Gossett, are adopted in accordance with this Memorandum and Order;
2. The Motion to Suppress filed by the Defendant Keith Noden, ECF No. 23, is denied; and
3. The Defendant Keith Noden's Objections to the Findings and Recommendation, ECF No. 33, are overruled.

Dated this 20th day of April, 2017.

BY THE COURT:

s/Laurie Smith Camp
Chief United States District Judge